FortiClient (iOS) v5.0 Patch Release 2
QuickStart Guide

FortiClient (iOS) v5.0 Patch Release 2 QuickStart Guide

December 03, 2013

04-502-198970-20131203

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2013-04-04	Initial release.
2013-12-03	Updated for FortiClient (iOS) v5.0 Patch Release 2.

Introduction

Thank you for choosing FortiClient for iOS.

FortiClient (iOS) is an secure web browsing and SSL VPN web-mode client that provides secure communications across the Internet to your network through secure socket layer (SSL) to ensure data privacy and security.

The FortiClient iOS app does not currently support IPsec VPN. You can use the Cisco IPsec VPN client which is built into your iOS device to connect to a FortiGate device. You can configure this VPN client in the iOS configuration profile (.mobileconfig), upload the profile to your FortiGate device, and deploy the configuration profile to your managed iOS device using the FortiGate endpoint control feature. See the *Mobile Configuration Profiles for iOS Devices Technical Note* for more information.

You can download FortiClient (iOS) v5.0 Patch Release 2 from the Apple App Store.

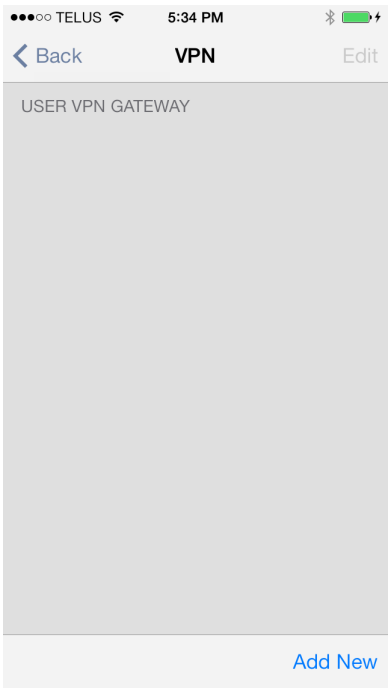
Initial Configuration

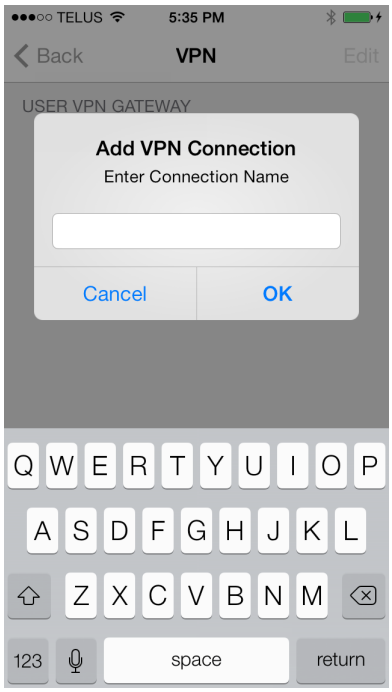
Create an SSL VPN connection without a client certificate

To create an SSL VPN connection without a client certificate:

1. When running the application for the first time, the browser is the default screen. Select the VPN icon in the FortiClient toolbar.
2. In *User VPN Gateway* select *Add VPN Connection.*
3. Enter a connection name and select *OK* in the dialog window. Each connection created must have an unique name.

Figure 1: User VPN Gateway and Add VPN Connection pages



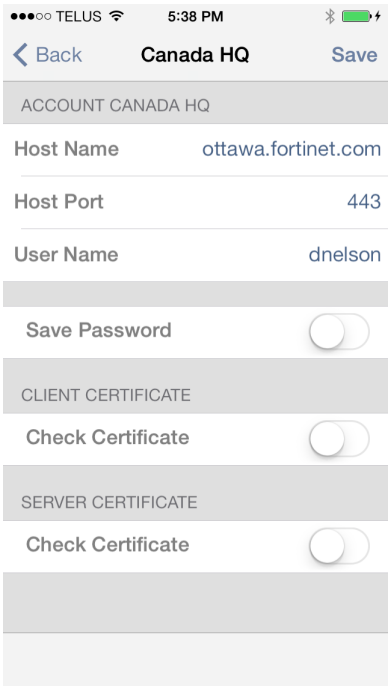


4. Select *Host Name,* enter the server host name or IP address, and then select *Done* in the keyboard menu.
5. Select *Host Port,* enter the server TCP port, and then select *Done* in the keyboard menu. The default port is 443.
6. Optionally, select *User Name* to enter user name and then select *Done* in the keyboard menu.
7. Toggle the *Save Password* value to *ON* if you want to save your password for this connection. The default value is *OFF*.

Saving connection passwords is not a recommended practice.

8. Toggle the *Server Certificate* switch to *ON* if you want to check the server certificate before connecting. The default value is *OFF.*

Figure 2: Account details page



9. Select *Save* in the toolbar to create the account.

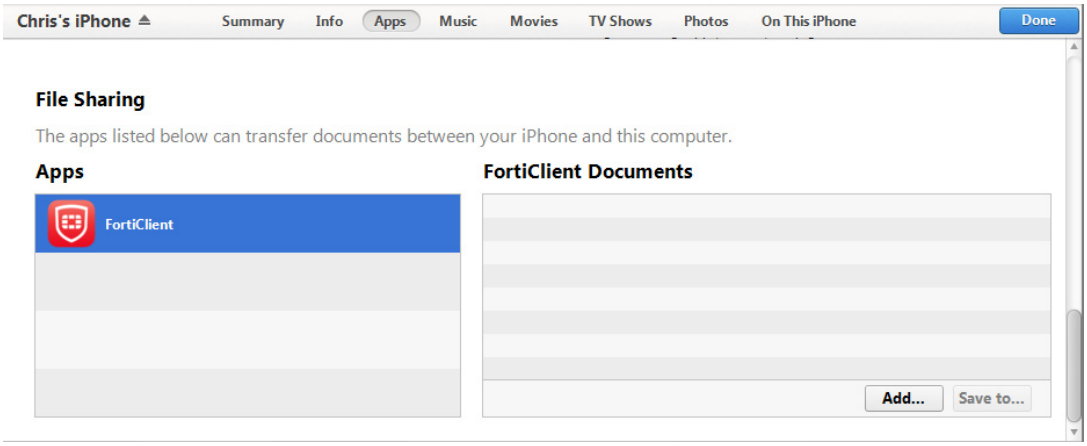
Configure client certificates

For more information, see the *Provision Certificates to iOS Devices Technical Note*.Optionally, you can view this document on the FortiClient application, browse to *Help* > *Documentation*.

To import certificates to the FortiClient application using iTunes:

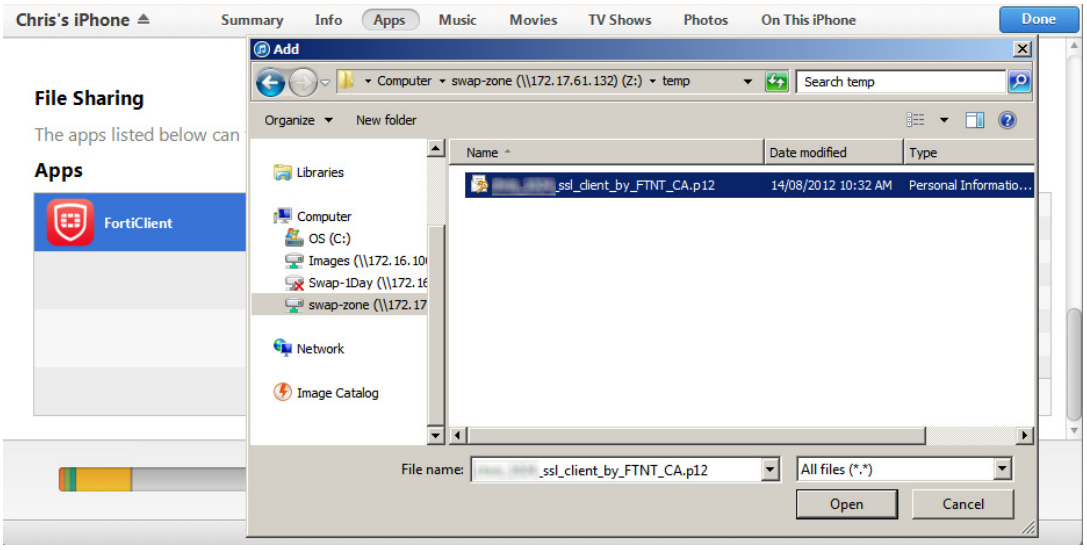
1. Open the iTunes program and connect your iOS device.
2. Browse to the iOS device home screen page and select *Apps*. Scroll down in the page to *File Sharing* and select the FortiClient icon in the Apps column.

Figure 3: iOS device home screen



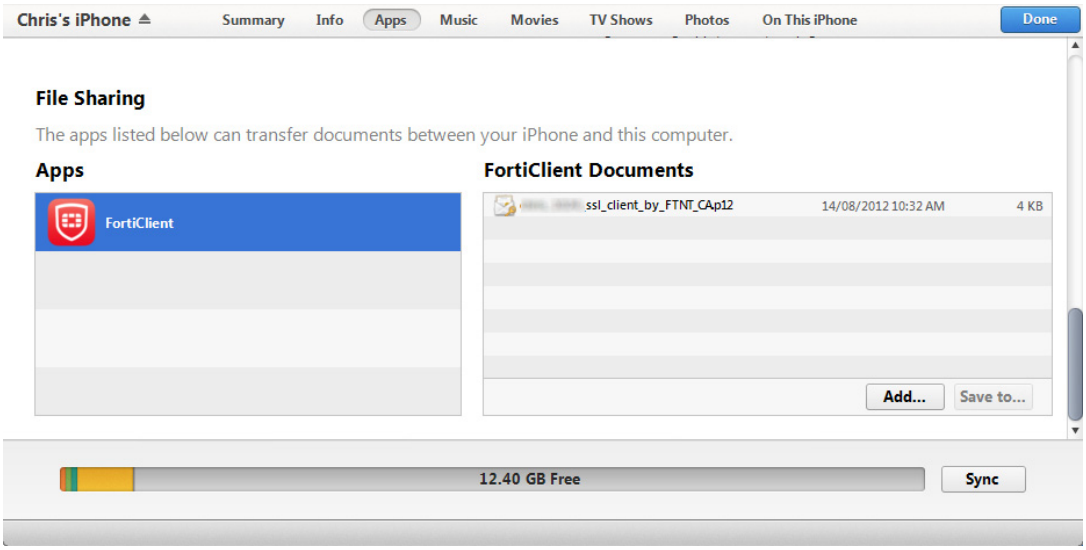
3. Select the *Add* button under *FortiClient Documents* and browse to you computers hard disk drive and locate the certificate file.

Figure 4: Browse to locate the certificate file



4. Select the certificate file and select *Open* to save it to the iTunes FortiClient document *File Sharing* directory.
5. Save to *File Sharing* directory and sync the iOS device with iTunes.

Figure 5: FortiClient documents

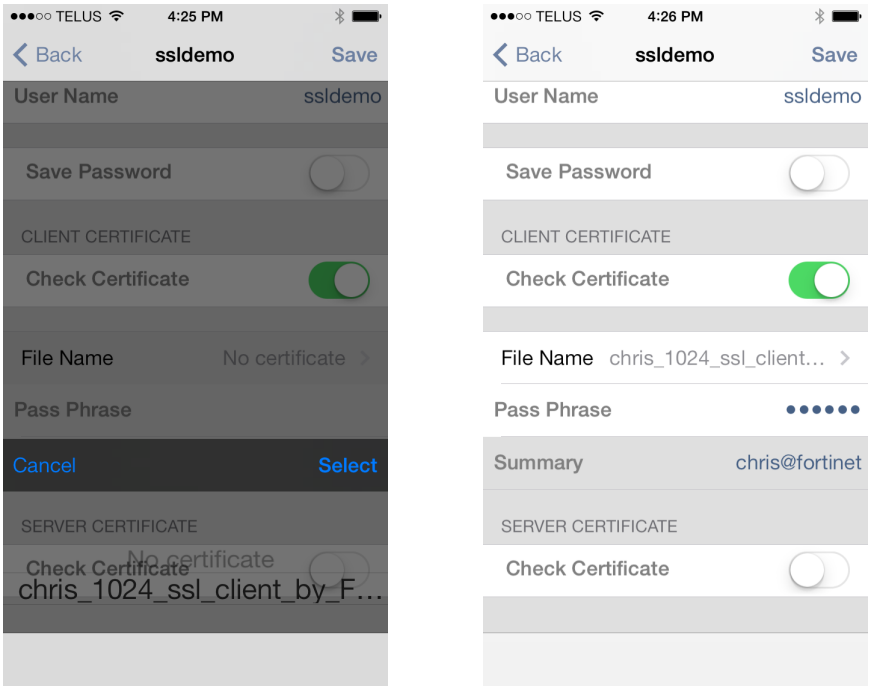


Configure certificates imported to iTunes

To configure certificates in the FortiClient application that have been imported using iTunes:

1. Open the FortiClient application, select the VPN icon in the toolbar, select *Edit* in the top menu pane, and select the VPN gateway you want to edit.
2. Under *Client Certificate* toggle *Check Certificate* switch to *ON.*
3. Select *File Name* and browse for the certificate you added in iTunes. Scroll to the certificate and then select *Select* to save the certificate to the FortiClient account.
4. Select *Pass Phrase*, enter the pass phrase for the certificate, and select *Done* in the keyboard menu.
5. If the *Pass Phrase* and the certificate are correct, the *Summary* field will display the certificate information.

Figure 6: Select the certificate pages



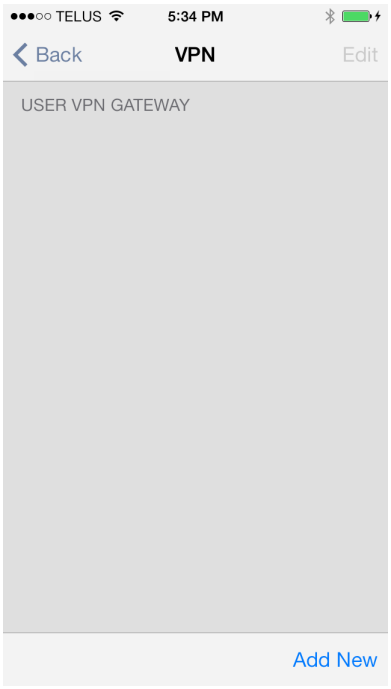
You can associate a certificate to each FortiClient connection.

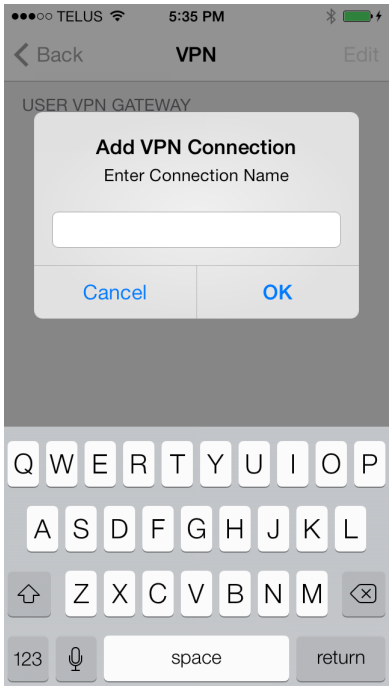
Create an SSL VPN connection with a client certificate

To create an SSL VPN connection with a client certificate:

1. When running the application for the first time, the browser is the default screen. Select the VPN icon in the FortiClient toolbar.
2. In *User VPN Gateway* select *Add VPN Connection.*
3. Enter a connection name and select *OK* in the dialog window. Each connection created must have an unique name.

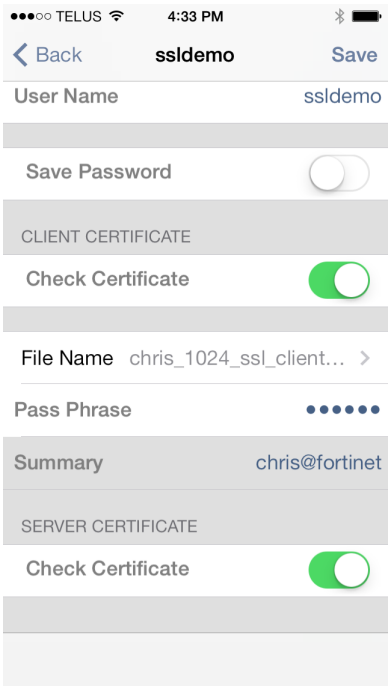
Figure 7: User VPN Gateway and Add VPN Connection pages





4. Select *Host Name,* enter the server host name or IP address, and then select *Done* in the keyboard menu.
5. Select *Host Port,* enter server TCP port, and then select *Done* in the keyboard menu. The default port is 443.
6. Optionally, select *User Name* to enter user name and then select *Done* in the keyboard menu.
7. Toggle the *Save Password* value to *ON* if you want to save your password for this connection. The default value is *OFF.*
8. Under *Client Certificate* toggle *Check Certificate* switch to *ON.*
9. Select *File Name* and browse for the certificate you added in iTunes. Scroll to the certificate and then select *Select* to save the certificate to the FortiClient account.
10. Select Pass Phrase, enter the pass phrase for the certificate, and select *Done* in the keyboard menu.
11. If the *Pass Phrase* and the certificate are correct the *Summary* field will display the certificate information.
12. Toggle the *Check Certificate* value in Server Certificate section to *ON* if you want to verify the server certificate. The default value is *OFF.*

Figure 8: Select the certificate pages



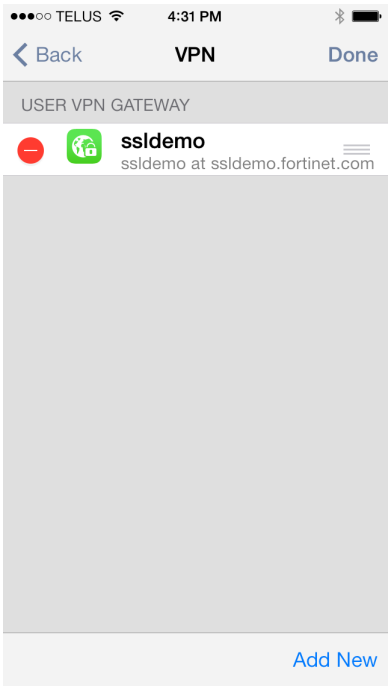
13. Select *Save* in the toolbar to create the account.

Edit or delete an account

To edit or delete an account, follow the steps below.

1. Select the VPN icon in the toolbar and select *Edit* in the top menu pane.
2. To edit an account, select the account from the list. Edit the fields as required, and select *Done* in the top menu pane to save the settings. You can also change the position of the entry in the list.

Figure 9: User VPN Gateway page



3. To delete an account, select the *red icon* to the left of the account and select delete.

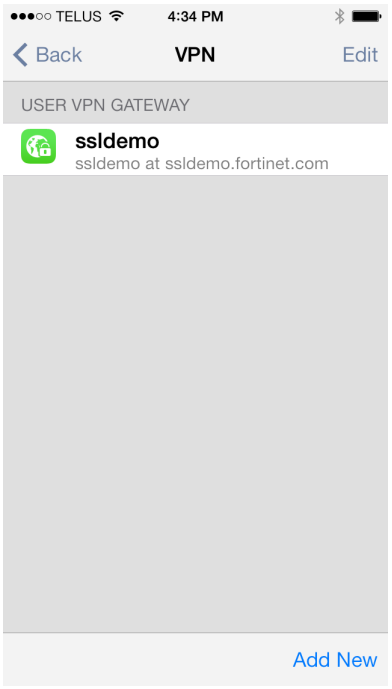
SSL VPN Connections

Starting an SSL VPN connection

To start an SSL VPN connection:

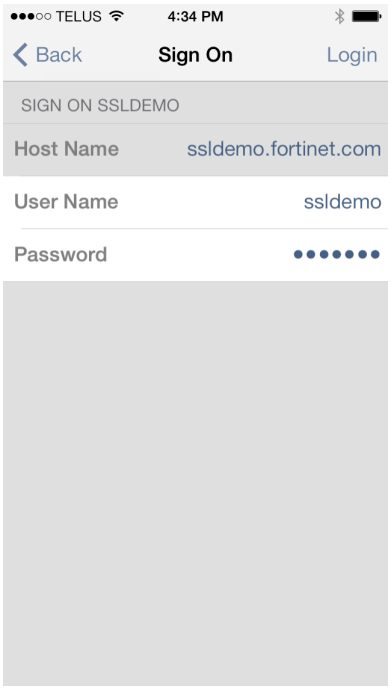
1. Select the VPN icon in the toolbar and select the account that you created for the VPN connection.

Figure 10: User VPN Gateway page



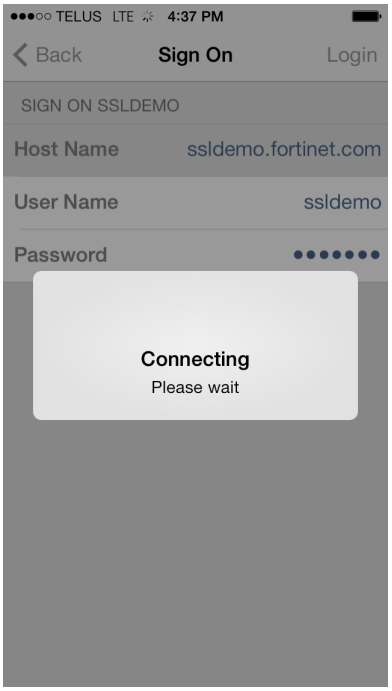
2. Select *Password*, enter your password, and select *Done* in the keyboard menu.

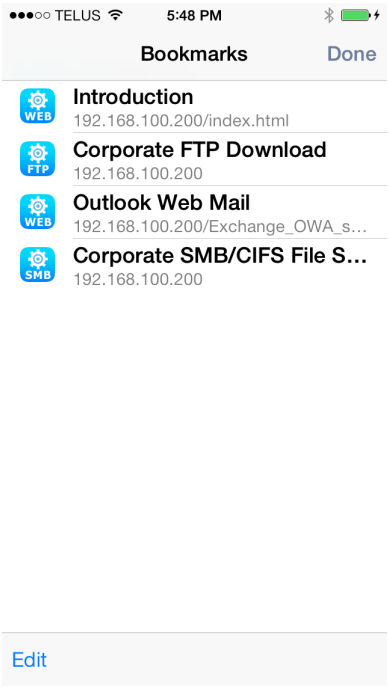
Figure 11: Select the account and enter your password



3. Select *Login* in the top menu pane. A connection window will display the connection status. Once the connection is established, you will be forwarded to the *Bookmarks* page.

Figure 12: Connection status and SSL VPN web portal pages





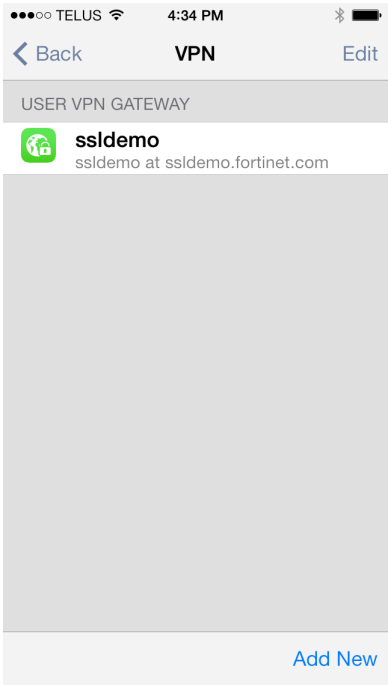
4. Select the bookmark from the list. To return to the *Bookmarks* screen, select the home icon in the top menu pane.
5. Select *Logout* to end the SSL VPN connection.

Start an SSL VPN connection using FortiToken

To start an SSL VPN connection using FortiToken:

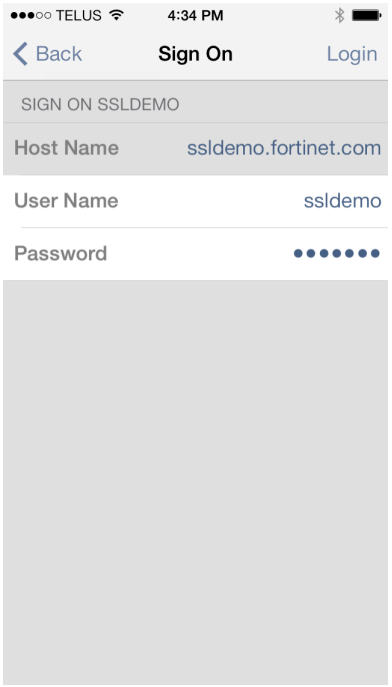
1. Select the VPN icon in the toolbar and select the account that you created for the VPN connection.

Figure 13: User VPN Gateway page



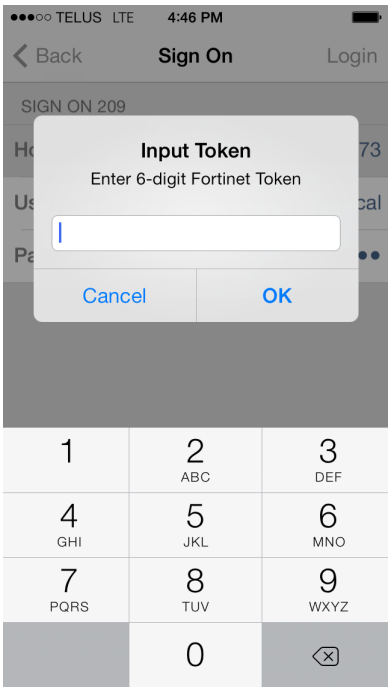
2. Select *Password*, and enter your password, select *Done* in the keyboard menu.

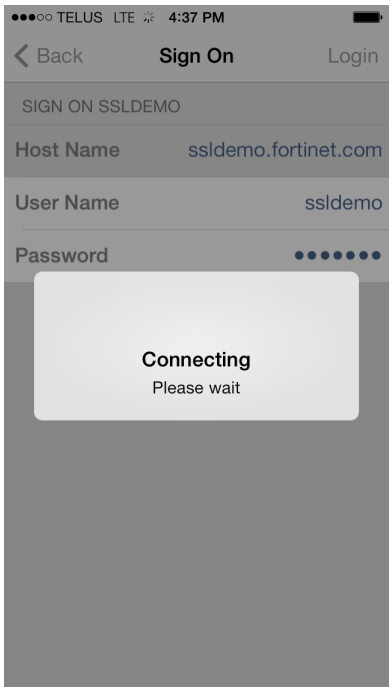
Figure 14: Select the account and enter your password



3. Select *Login* in the top menu pane.
4. Enter your 6-digit FortiToken value displayed on your FortiToken in the *Input Token* pop-up window and select *OK*. A connection window will display the connection status.

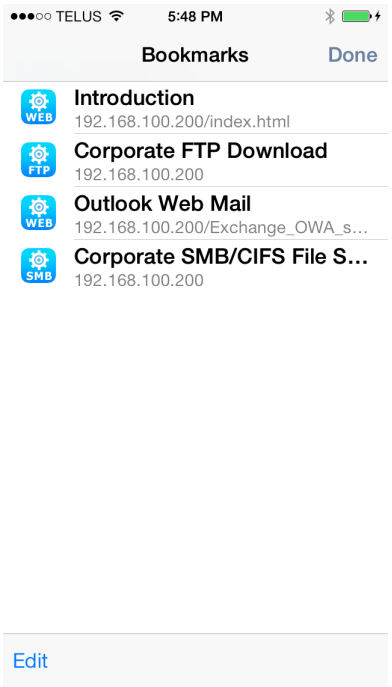
Figure 15: Token and connection status page





5. Once the connection is established, you will be forwarded to the SSL VPN web portal page where you can access pre-defined *Bookmarks*.

Figure 16:SSL VPN web portal page



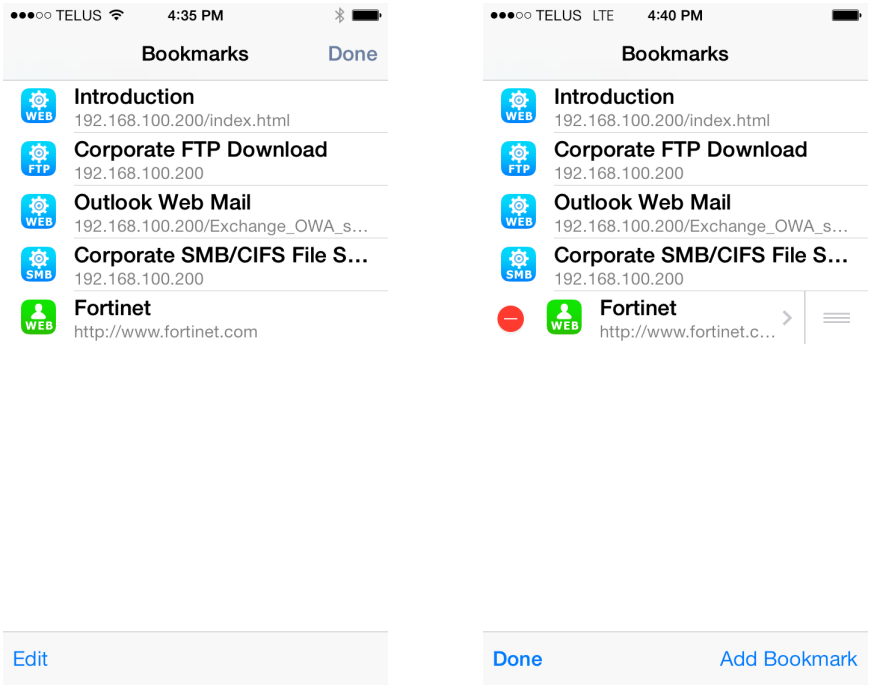
6. Select the bookmark from the list. To return to the *Bookmarks* screen, select the home icon in the top menu pane.
7. Select *Logout* to end the SSL VPN connection.

User Bookmarks

To add user bookmarks:

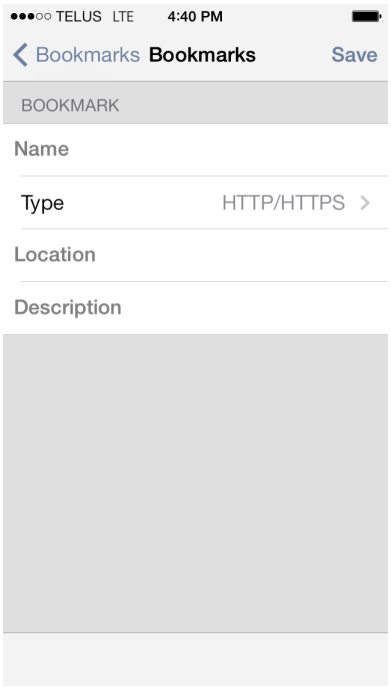
1. Login to the SSL VPN web portal. Select *Edit* in the toolbar and then select *Add Bookmark*. You can also edit bookmarks and change their position in the list. If user bookmarks are not allowed, these buttons will not be available.

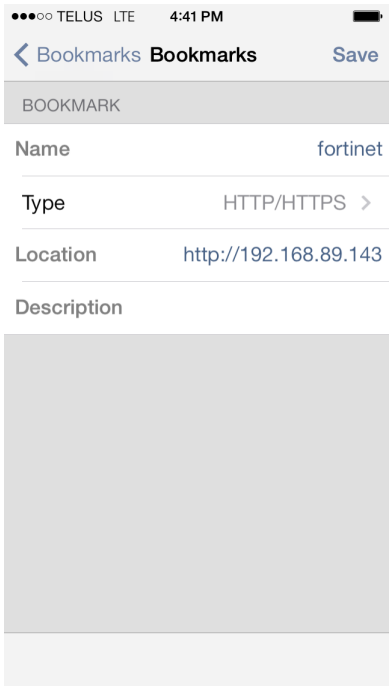
Figure 17:SSL VPN web portal pages



2. Select *Name* to enter bookmark name, and then select *Done* in the keyboard menu.
3. Select *Type* to select bookmark type, and then select *Done* in the keyboard menu.
4. Select *Location* to enter bookmark URL, and then select *Done* in the keyboard menu. You can select *Description* to enter bookmark description (optional).

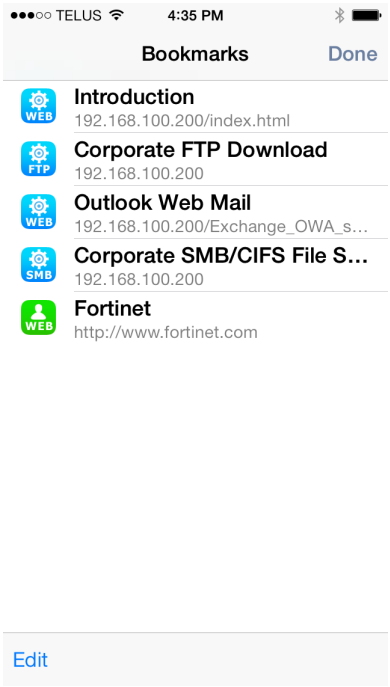
Figure 18: Add Bookmark pages





5. Select *Save* in the top menu pane to save the setting.

Figure 19: User Bookmark added successfully



6. Select *Done* in the toolbar when you are finished adding bookmarks.

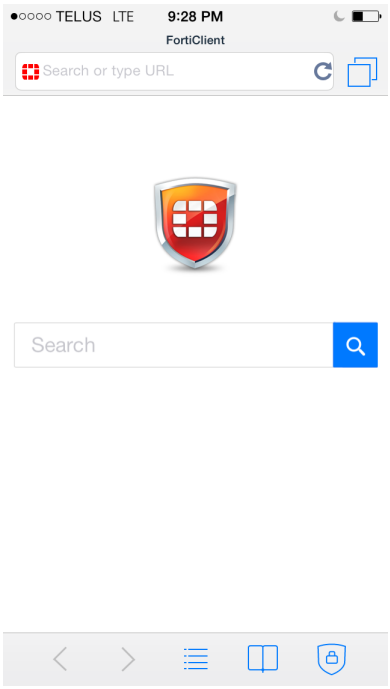
Secure Web Browsing

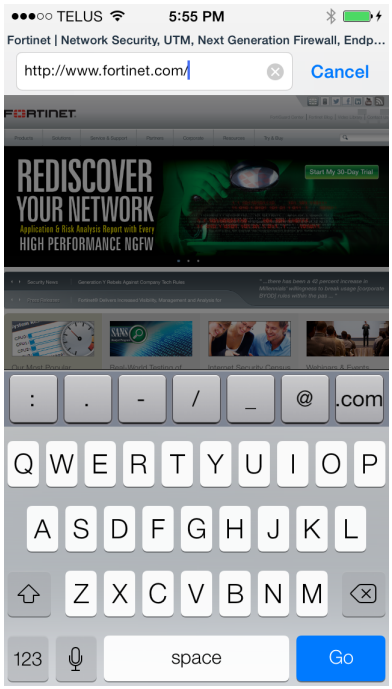
Browsing the Internet with the secure web browser

To browse the Internet:

1. To browse to a web site, enter the URL in the address field. The web browser has a built-in Google search field. To navigate backwards or forwards through the browser history, use the left and right directional arrow icons in the button bar.

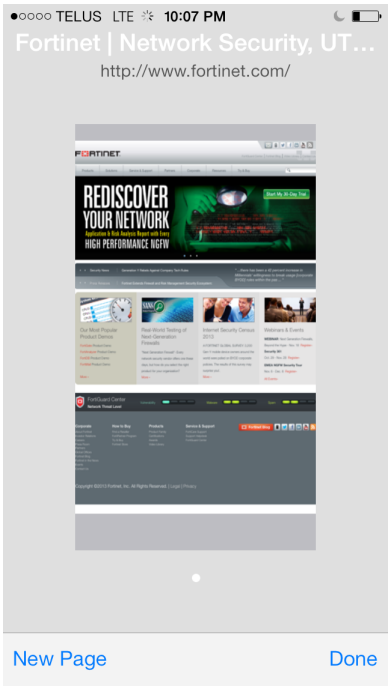
Figure 20: Secure web browser page





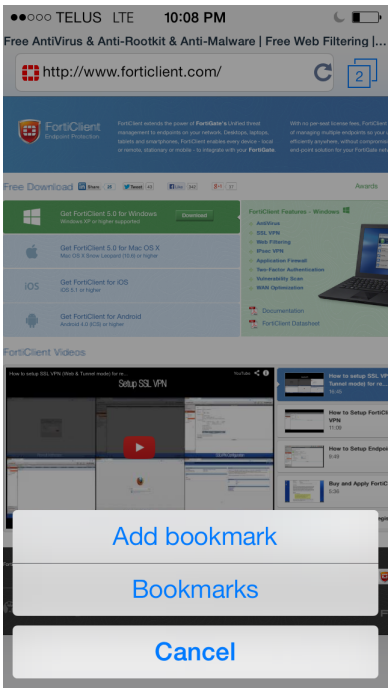
2. To add a new browser window, select the icon to the right of the address field and select *New Page* in the toolbar. Select this icon to switch between pages.

Figure 21: Add a new page



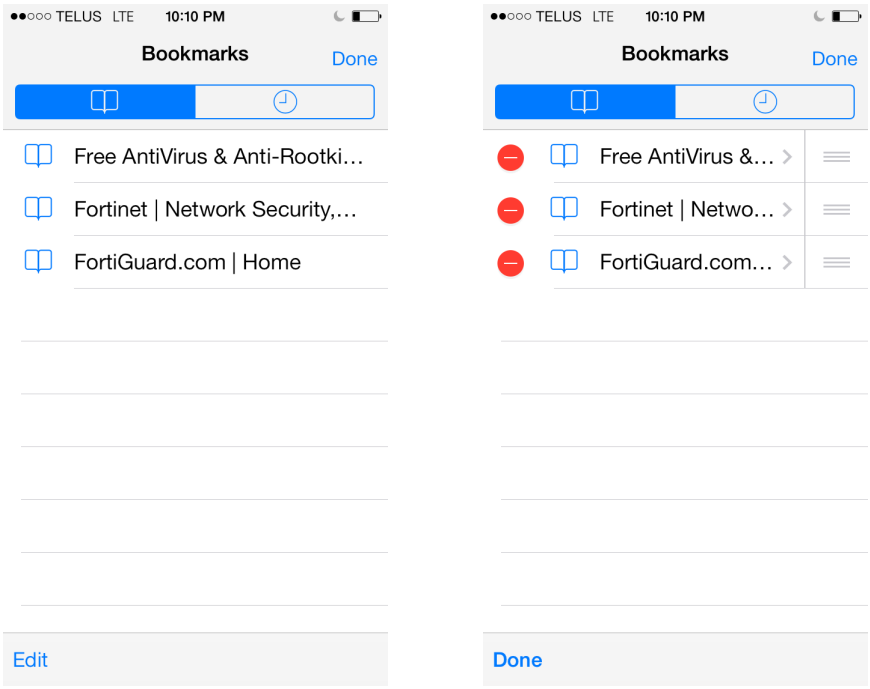
3. To add a bookmark for the current web page, select the add bookmark icon in the toolbar, and then select *Add bookmark*. You also have the option to mail the link to this web page.

Figure 22: Add a bookmark



4. Select the bookmark icon in the toolbar to view saved bookmarks. Select *Edit* to edit these bookmarks and change the position of bookmarks in the list.

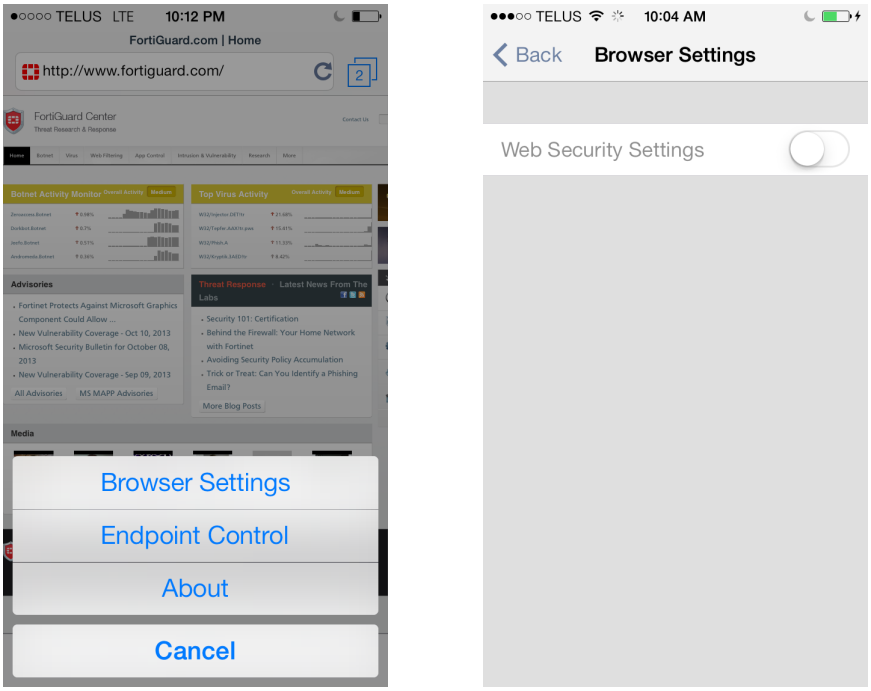
Figure 23: Bookmark pages



Configure web browser restrictions

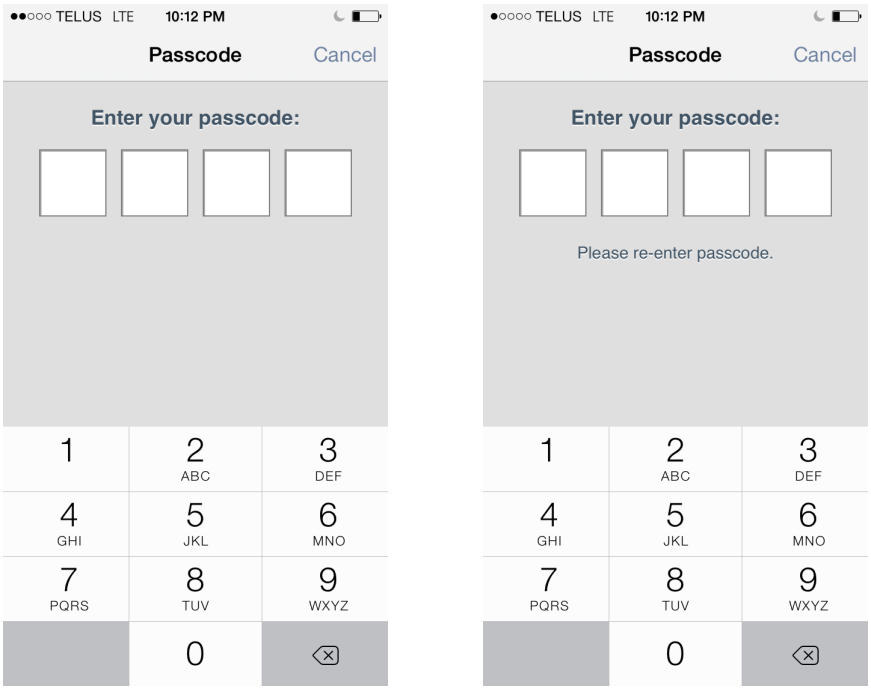
1. Select the settings icon in the toolbar and select *Browser Settings*.

Figure 24: Enable web restrictions page



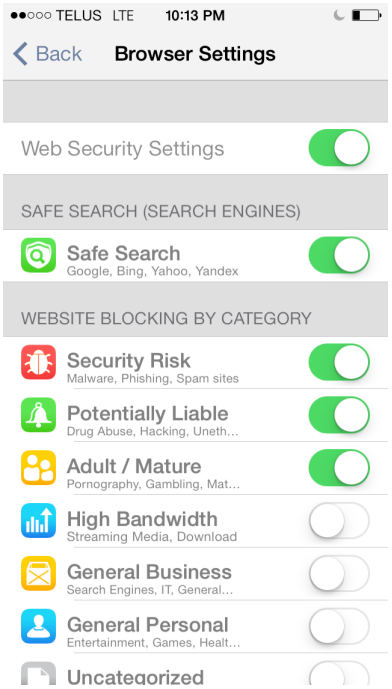
2. Select *Enable Web Restrictions* and enter a new four-digit passcode to activate this feature. You will be prompted to confirm the passcode. The passcode will be required to make changes to web restrictions and to disable the feature.

Figure 25: Passcode pages



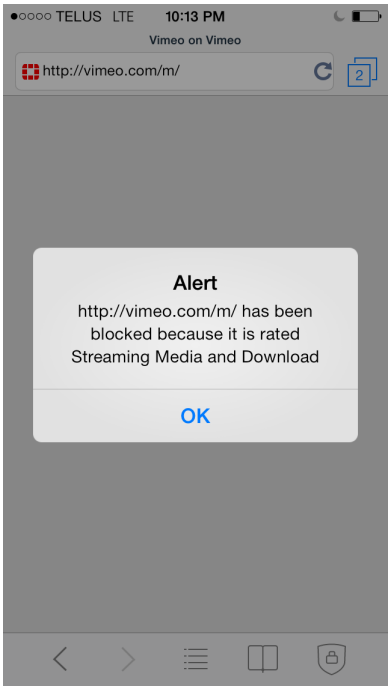
3. To block web categories, toggle the switch to *ON*. To allow access to web categories, toggle the switch to *OFF*. Select *Disable Web Restrictions* to disable this feature. You will be required to enter the passcode continue. Browser settings can also be configured in the endpoint control profile. See “FortiGate Endpoint Control” for more information.

Figure 26: Toggle to block or allow web categories



4. Select the *Back* button in the toolbar to return to the secure web browser. When browsing to a web page that belongs to a blocked category, the user will receive an alert message with details why the site was blocked.

Figure 27: Web page blocked alert



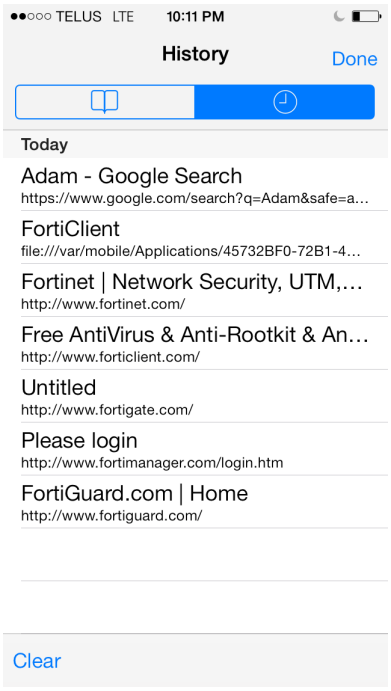
5. To edit web browser settings, select the settings icon in the toolbar and select *Browser Settings*. Enter your passcode to made changes.

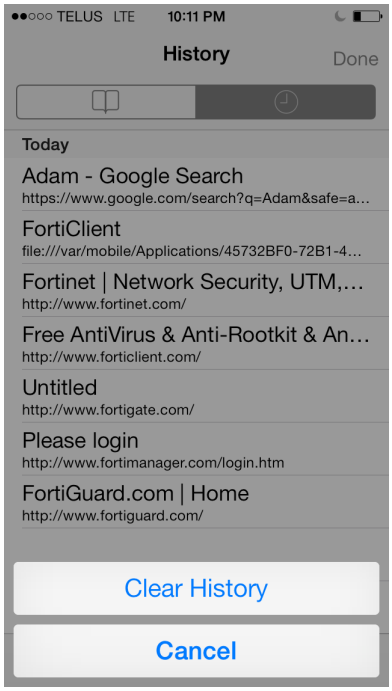
If you forget the *Web Restrictions* passcode, you will need to delete, and re-install the application.

View and clear browser history

FortiClient (iOS) v5.0 Patch Release 2 allows you to view and clear the web browser history. The browser history feature provides URL suggestions when you enter a URL.

Figure 28: View and clear browser history



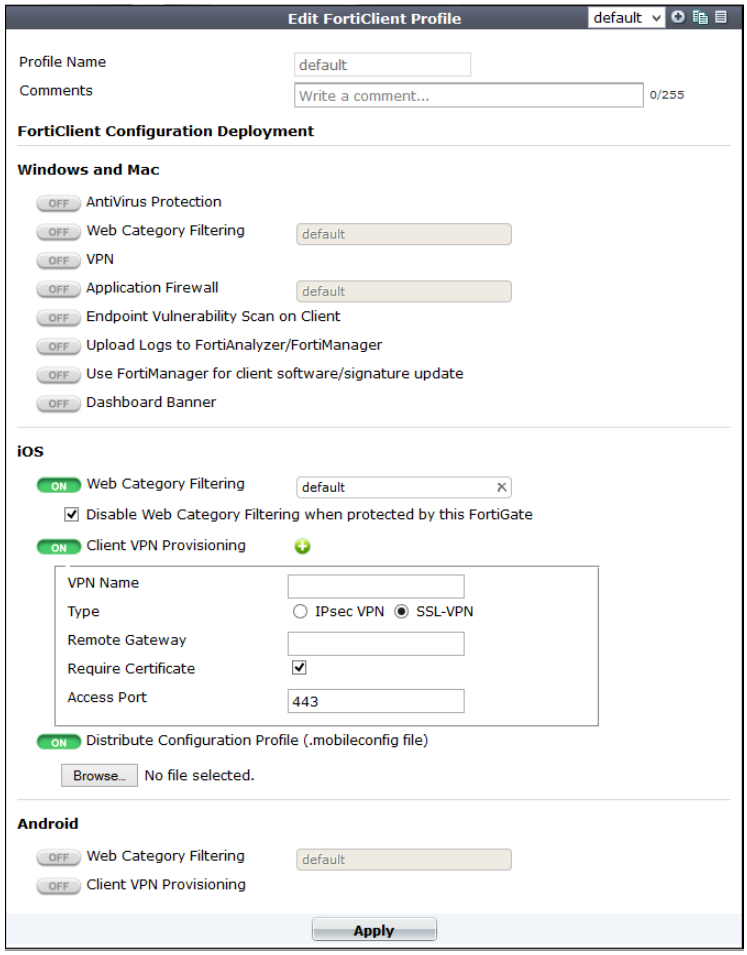


FortiGate Endpoint Control

In FortiOS v5.0 Patch Release 2 or later you can deploy a FortiClient Profile to your FortiClient iOS devices. The profile can include *Web Category Filtering* configuration, *Client VPN Provisioning*, and you can distribute a *.mobileconfig* file to registered clients. See the *Mobile Configuration Profiles for iOS Devices Technical Note* for more information on configuring .mobileconfig profiles.

The iOS FortiClient Profile is configured on your FortiGate device, see Figure 29. You can configure a .mobileconfig profile using the iPhone Configuration Utility, the Apple Configurator app, or Mac OS X Server Profile Manager. When uploaded to the FortiGate FortiClient Profile, this mobile configuration file will be distributed to Managed FortiClient iOS devices.

Figure 29: FortiGate iOS FortiClient profile

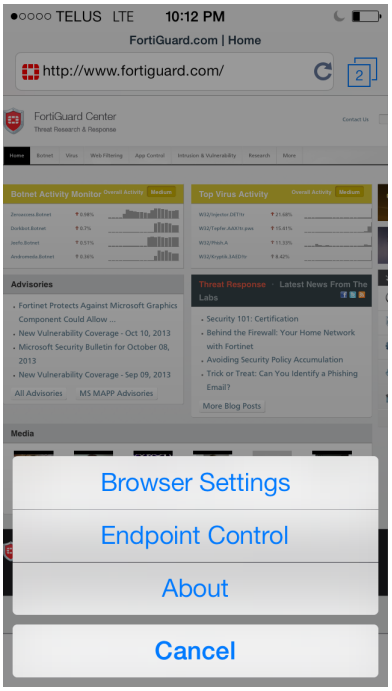


The FortiClient iOS app does not currently support IPsec VPN. You can use the Cisco IPsec VPN client which is built into your iOS device to connect to a FortiGate device. You can configure this VPN client in the iOS configuration profile (.mobileconfig), upload the profile to your FortiGate device, and deploy the configuration profile to your managed iOS device using the FortiGate endpoint control feature. See the *Mobile Configuration Profiles for iOS Devices Technical Note* for more information.

Enable FortiGate Endpoint Control

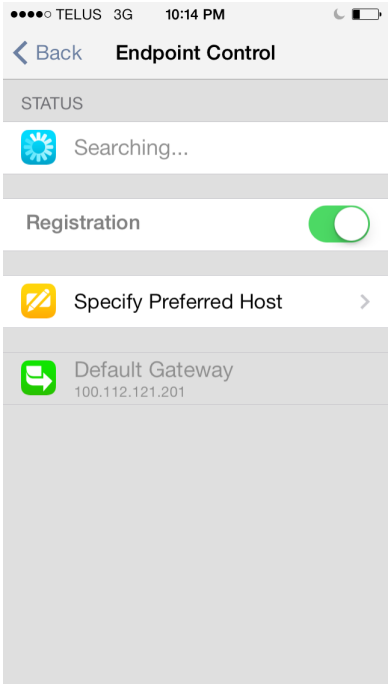
1. Select the settings icon in the toolbar and select *Endpoint Control*.

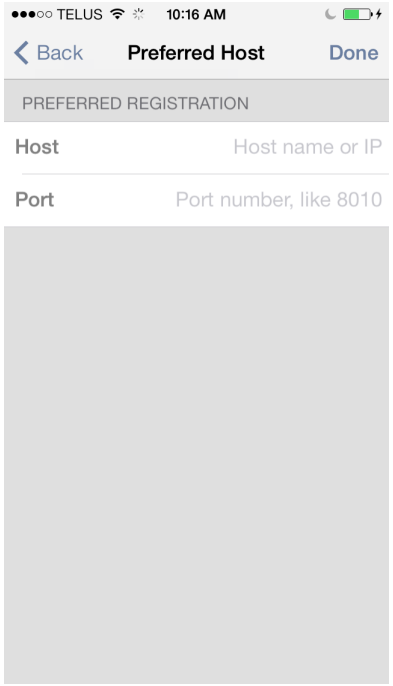
Figure 30: Settings menu



2. Toggle the *Registration* switch to *ON*. FortiClient iOS will search for the FortiGate device. Optionally, you can select *Specify Preferred Host* and enter the host name or IP and port information in the *Preferred Registration* page.

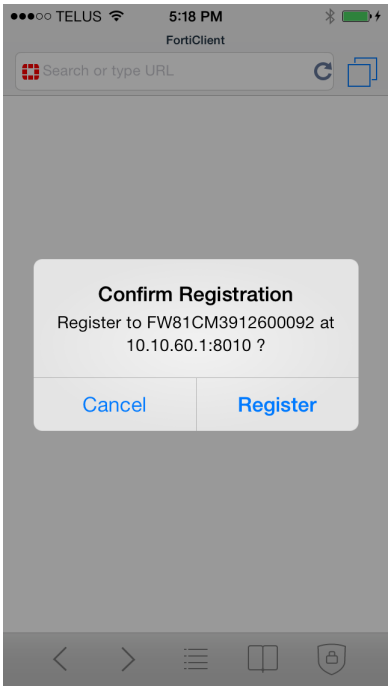
Figure 31: FortiClient Endpoint Control page

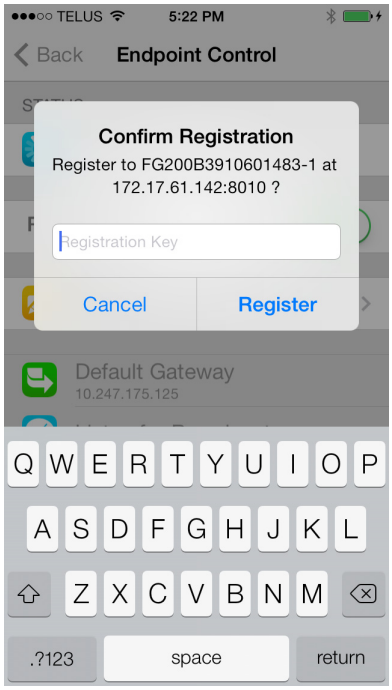




3. You will receive a *Confirm Registration* pop-up dialog box. Select *Register* to complete registration with the FortiGate. Optionally, you may be required to enter a registration key. Contact your network administrator for the registration key.

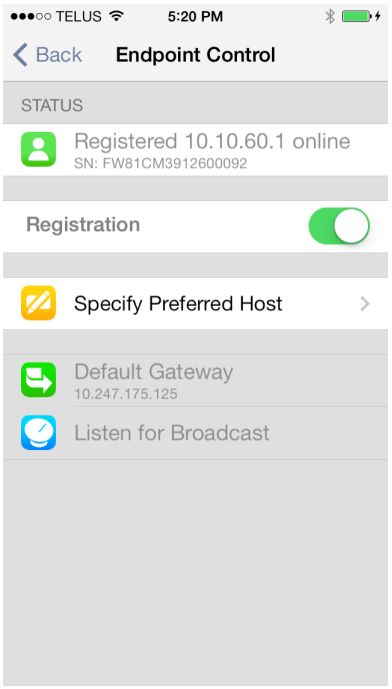
Figure 32: Registration pop-up windows





4. FortiClient iOS will display the registration information in the *Status* page.

Figure 33: Registration status page

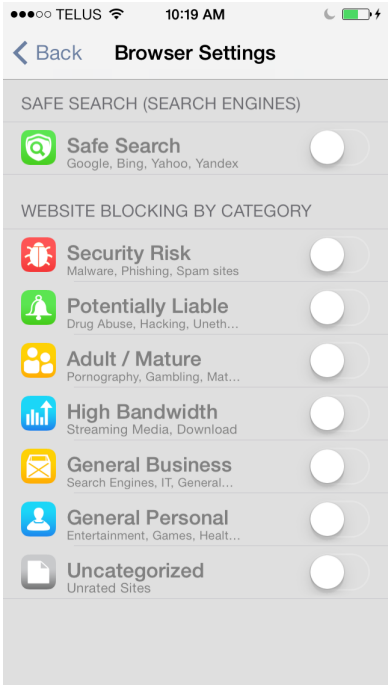


If the FortiGate device has reached the maximum number of registered FortiClient endpoints, you will receive a pop-up notification dialog box.

Web browser settings

When web browser settings are configured in the FortiGate FortiClient Profile, *Browser Settings* are read-only and cannot be edited by the end user.

Figure 34: Browser settings page

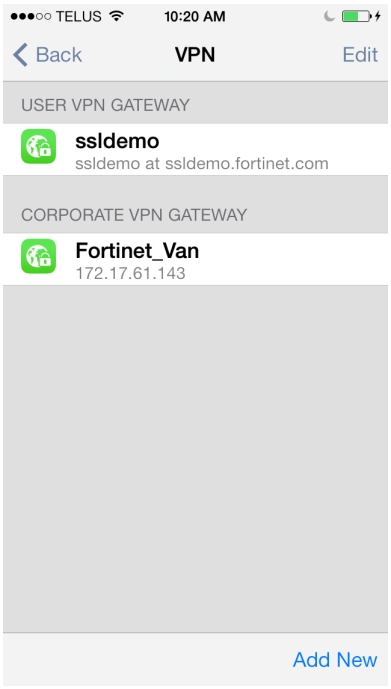


Alternatively, you can configure web browser settings per device. See “Secure Web Browsing” for more information.

VPN Provisioning

You can configure multiple IPsec and SSL VPN configurations in the FortiClient iOS endpoint profile including the *Corporate VPN Gateway*. See the *FortiGate 5.0 Handbook* for more information on configuring VPN connections.

Figure 35: Corporate VPN Gateway example

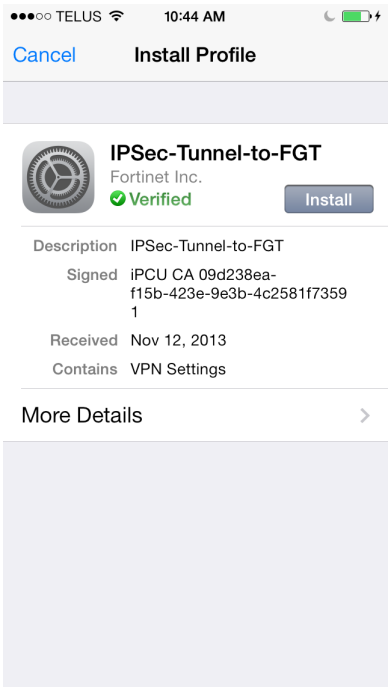


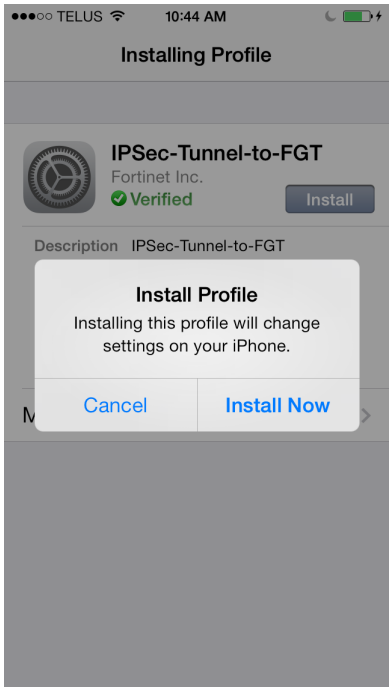
Deploy the iOS FortiClient Profile to FortiClient iOS

You can deploy the FortiClient Profile over the *Corporate VPN Gateway* connection.

1. Select the *VPN* icon in the toolbar, and select the *Corporate VPN Gateway* connection. Enter the password for the VPN profile.

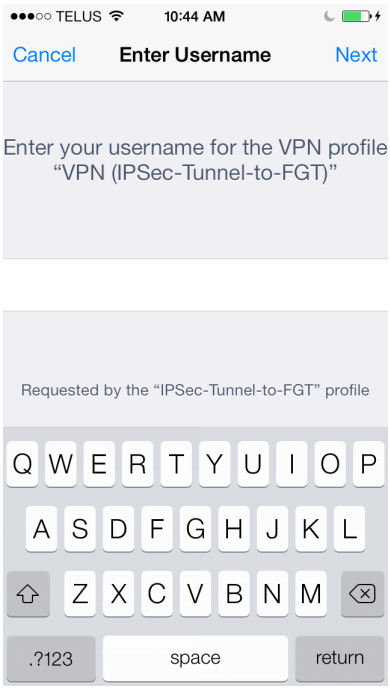
Figure 36: Corporate VPN Gateway page

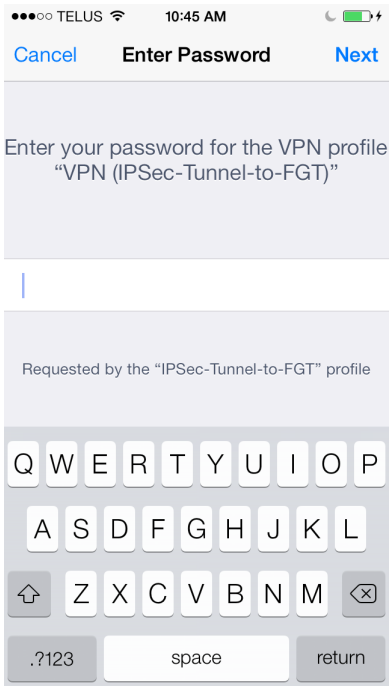




2. When connected you will be prompted to install the FortiClient Profile on your iOS device. Select *Install* in the *Install Profile* page and *Install Now* in the pop-up window.

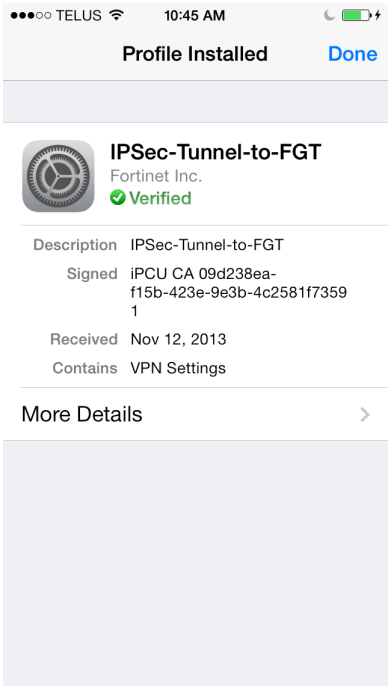
Figure 37: Install profile pages





3. The profile will be installed on your device. Select *Done* in the *Profile Installed* page to proceed.

Figure 38: Profile installed page



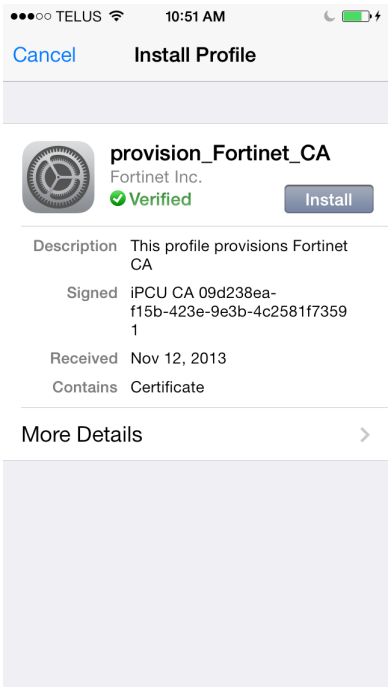
4. You can now proceed to use FortiClient iOS.

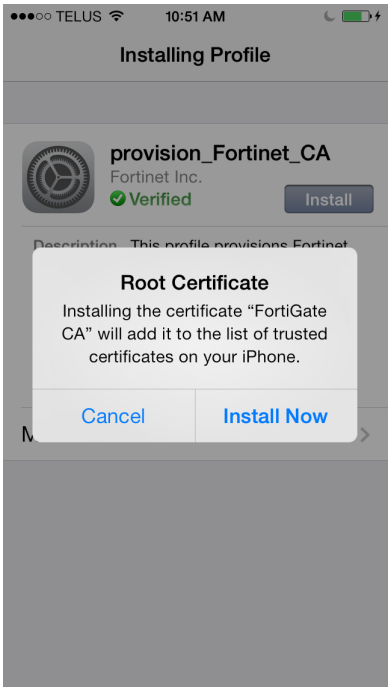
Deploy a certificate over endpoint control

You can deploy CA certificates over endpoint control to your iOS devices. See the *Provision Certificates to iOS Devices Technical Note* for more information.

When the certificate is deployed to iOS devices, the user will be prompted to install the certificate. Select *Install* in the *Install Profile* page and *Install Now* in the pop-up window.

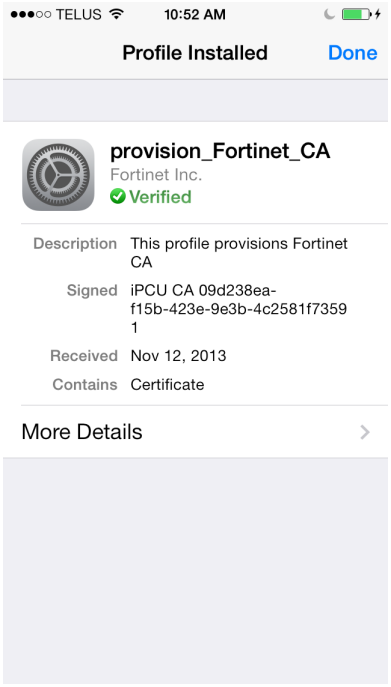
Figure 39: Install certificate windows





The certificate will be installed on your device. Select *Done* in the *Profile Installed* page to proceed.

Figure 40: Certificate installed page



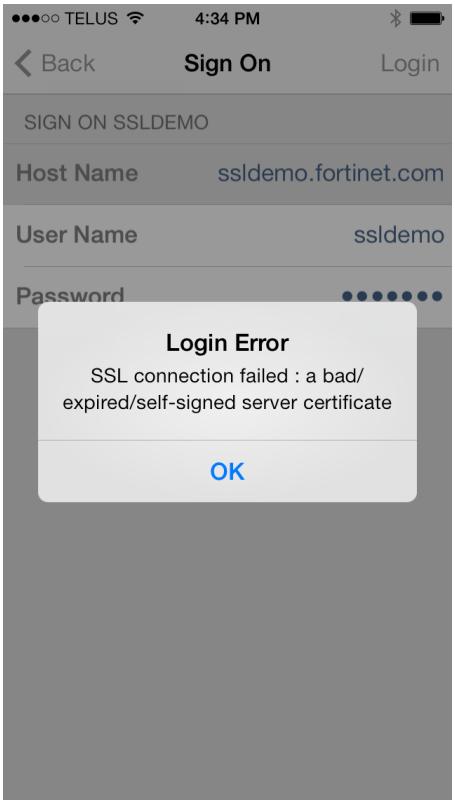
You can now proceed to use FortiClient iOS.

Appendix A: Troubleshooting

Invalid server certificate

If the server certificate is untrusted, the user will receive the following error message: *Login Error: Connection failed: SSL Problem: possibly a bad/expired/self-signed server certificate.*

Figure 41: Login Error window



To resolve this issue:

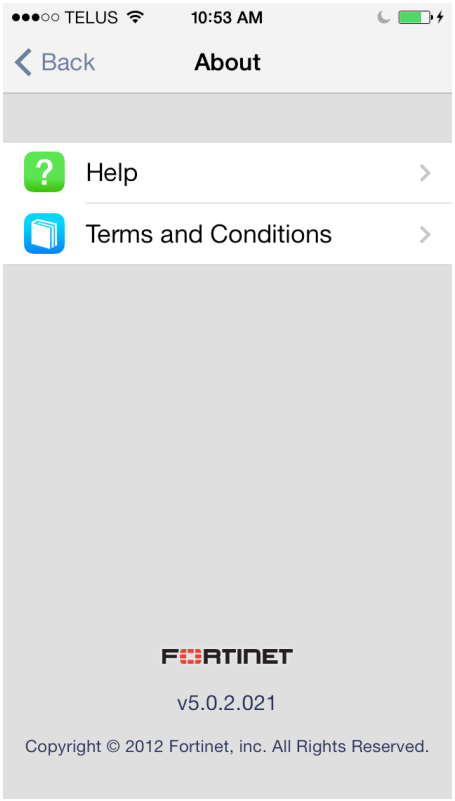
1. Select the *VPN* icon in the toolbar.
2. Select the *Edit* button in the top menu pane.
3. Select the *User VPN Gateway* that you are using for the connection.
4. Toggle the *Check Certificate* value in *Server Certificate* section to *OFF* to not verify the server certificate.
5. Select *Save* in the top menu pane.
6. Start a new connection.

Appendix B: Additional Information

Information page

The settings icon allows you to access browser settings, endpoint control settings, and additional information including *Help*, and *Terms and Conditions*.

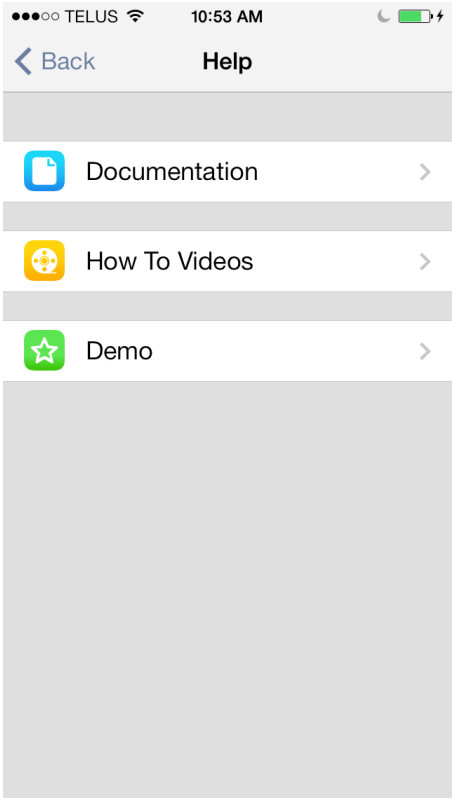
Figure 42: About page



Help menu

The *Help* menu allows you to access FortiClient iOS documentation, how to videos, and a SSL VPN demonstration.

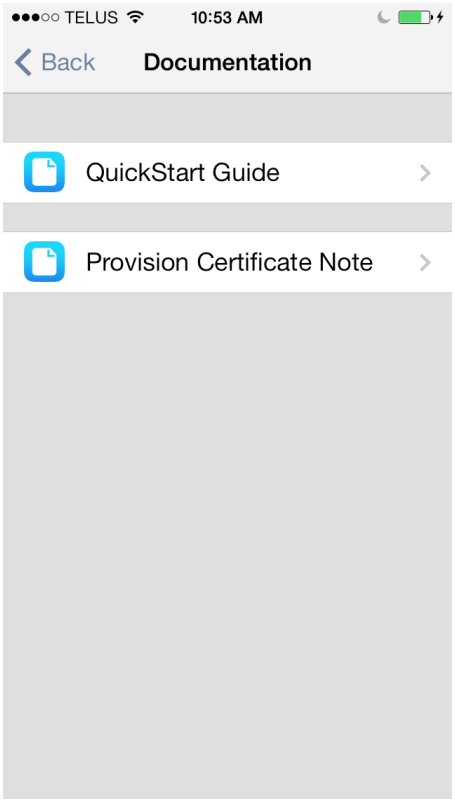
Figure 43: Help menu page



Documentation menu

Documentation includes the *FortiClient QuickStart Guide*, and the *Provision Certificates to iOS Devices Technical Note*.

Figure 44: Documentation page



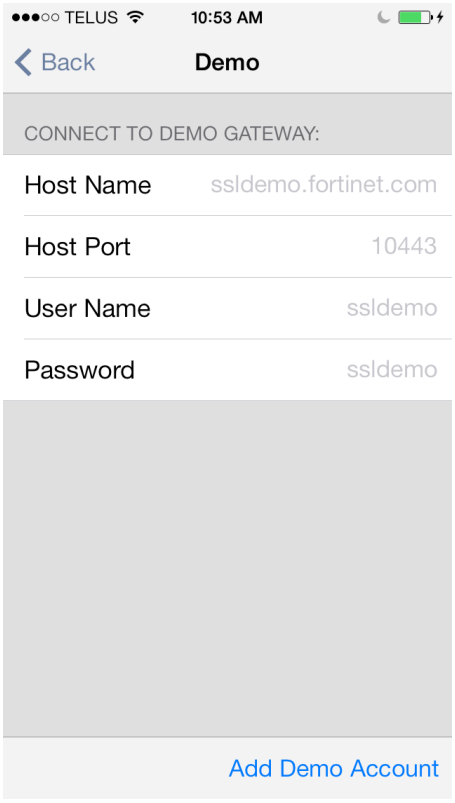
How To Videos

A video has been provided to walk you through the FortiClient SSL VPN client.

SSL VPN Demo

To connect to the SSL VPN demonstration, select *Help* in the settings page, and then select *Demo* in the *Help* page. Select *Add Demo Account*, to add the account. The demo allows you to test SSL VPN features.

Figure 45:SSL VPN demonstration page



Terms and Conditions

Terms and Conditions forward you to the *Fortinet Product License Agreement, EULA, and Warranty Terms, Trademarks and Copyright Statements* page.

Figure 46: Terms and Conditions page